May 18, 2016

Filed electronically

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

I respectfully submit the attached Comment for the above-referenced matter. Please let me know if you have any questions.

Sincerely,

Shawn Sheridan
Turlock, California

Attachment

cc (via email): David Brody, Matt DelNero, Lisa Hone, Scott Jordan, Daniel Kahn, Melissa Kirkel, Travis Litman, Charles Mathias, Bakari Middleton, Ruth Milkman, Sherwin Siy, Jennifer Tatel, Jon Wilkins

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106
	)	

COMMENT

Filed: **May 18, 2016**

By: Shawn Sheridan
290 N. Thor St., Apt. 200
Turlock, CA 95380-4000
sheridan3398@yahoo.com

TABLE OF CONTENTS

I. DECLARATION

1. I declare under penalty of perjury under the laws of the State of California that the following is true and correct:

My personal experiences mentioned in this Comment and filings for MB Docket 15-149.[1]

I am a former subscriber to video, voice or Internet services.

I am indigent—my gross monthly income is less than 300% of federal poverty guidelines.

I am not an expert, scholar, lawyer or representative; but a researcher and free-thinker can also provide assistance.

I am the author of this Comment.

Date executed: May 18, 2016

Place: Turlock, California; County of Stanislaus

Signature: */s/ Shawn D. Sheridan*
Shawn D. Sheridan

II. INTRODUCTION

2. For me it is now abundantly clear that some in the U.S. Intelligence Community have followed my comments and letters filed for MB Docket 15-149 pertaining to surveillance and long-term activities to place viruses and files on my personal laptop. It wasn't until I read the Commission's Notice of Proposed Rulemaking (NPRM or Notice) that I learned of the existence of the Communication Assistance for Law Enforcement Act (CALEA), which became law one year before my typewriter, which was central on my desk at work, was replaced with a personal computer. And it wasn't until a year more, in 1996, that I first accessed the Internet.

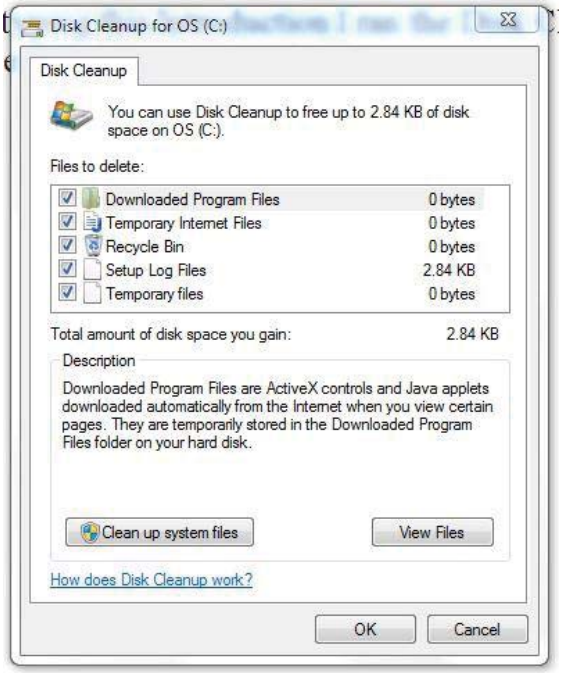
3. Recognizing that my privacy has been violated by daily surveillance/technology equipped planes flying over my locations at least since October 2015—documented in my filings to the Commission via MB Docket 15-149[2]—I have been forced to ask serious questions about my safety and privacy. Apparently my privacy has not been legally violated, but it most certainly has been morally violated.

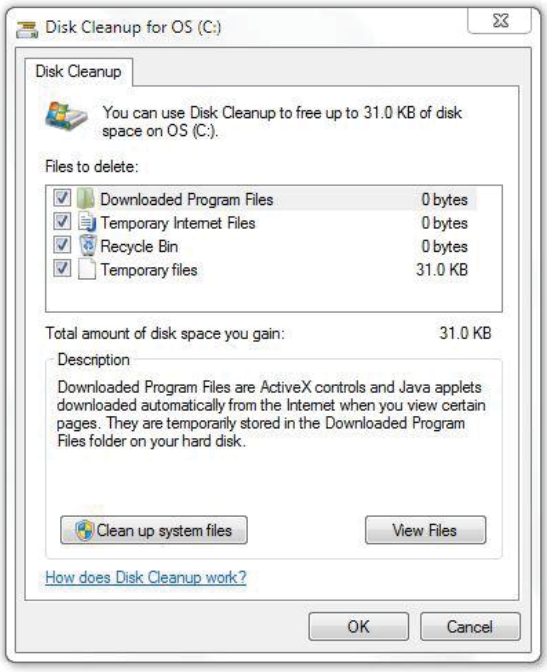
4. I will provide the Commission four more examples of what I have experienced. Either on the night of when the FCC publicized approval of the Charter/Time Warner merger,[3] or the next night, I was outside of a closed library accessing the Internet with my iPad. About ten to fifteen minutes later I heard and then saw a helicopter hover and slowly fly extremely low two blocks away. I turned off Wi-Fi then the device, but when I turned the device back on, after the helicopter could no longer be heard and after a plane flew over, my iPad went into setup mode as though it had been reset. I turned the iPad on and off three times and the setup screen remained, but when I swiped through the first two to three setup screens the iPad opened as though nothing had occurred.

5. Another incident occurred in the afternoon of Sunday, May 8, when I again stood outside a closed library accessing the Internet with my iPad. A familiar helicopter with "Sheriff" written on the side circled just above the trees either three or four times, and it felt exactly like a movie as though vans were about to show up. The helicopter then flew directly to my residence four blocks away. When I returned home, my mother said the helicopter circled the apartment *three times* as she stood outside watching.

6. A third example, among many, many incidents that could be mentioned, occurred on Monday, May 9, when a familiar white plane flew low and extremely slow over my residence as my mother and I walked outside to get in her car. We went to my sister's house a few miles away, and the same or identical plane flew directly over my sister's house at the same altitude and speed as we were getting out of the car at her house.

7. As I was typing this introduction I ran the Disk Cleanup tool, like I regularly have for months, and the following appeared. 'They' have inserted many different files while flying over as either a setup log file, temporary file or temporary Internet file, but I just delete the file(s) before continuing.[4] The second image occurred at a later time as I was typing this document on May 13, but both are examples of countless insertions while not connected to the Internet.





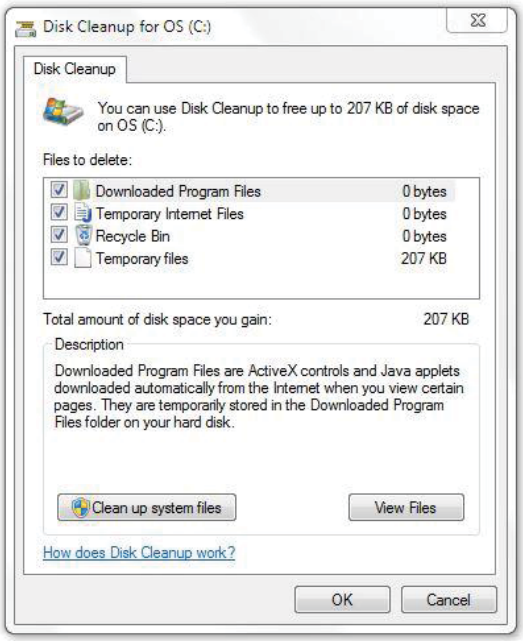
(Beginning from previous page) ———————————————

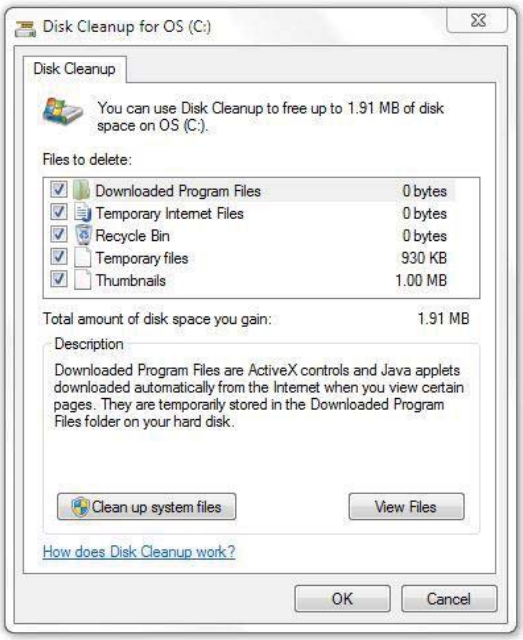
[1] In the Matter of Applications of Charter Communications, Inc., Time Warner Cable Inc., and Advance/Newhouse Partnership for Consent to Transfer Control of Licenses and Authorizations.

[2] *See* Oct. 17, 2015 Letter; Nov. 12, 2015 Reply to Responses/Oppositions at 31; Dec. 27, 2015 Supplemental Reply to Responses/Oppositions at 23; Jan. 19, 2016 Additional Reply to Responses/Oppositions at 12; Feb. 4, 2016 Letter; April 11, 17 and 27, 2016 Letters for MB Docket 15-149.

[3] FCC 16-59, released May 10, 2016.

8. The following are two more insertions that took place shortly after the 31 KB file mentioned above. There was such as onslaught of files being inserted for two to three minutes as I continued to run Disk Cleanup[5] that I only spent time screen-printing the following:





9. Not only am I forced to ask what legal authorization exists for such activities, but I am forced to assume that I have something to say. Beginning after my comments were filed at fcc.gov last September, I was somehow deemed suspicious or a threat so that a police helicopter has flown overhead on multiple occasions and yet no police officer has ever come to my door. What has been occurring has nothing to do with enforcement of law, but rather espionage.

10. My predicament has forced me to ponder things like how lucrative I must be as a target for a third party involved in the surveillance. At this point, it seems obvious that part of the government is active in the complot. So part of the government likely has me under surveillance as I comment to another part of the government pursuing privacy protections.

11. I wonder, was the *Notice* produced because of issues concerning mostly legality, morality or ethics? Did the Commission dismiss government surveillance because of existing law or simply choice? Because the *Notice* contains hundreds of considerations in which comment is sought, but the only elephant in the room was conspicuously relegated.

(Continued from previous page) ————————————————

[4] What may seem irrelevant, such as a 2.84 KB file, is just one of countless attempts to inject a crack into my laptop because I have so many Windows 7 and other system settings disabled when not accessing the Internet; perhaps to frustrate me, harm my laptop, and/or covertly retrieve information, such as a screenshot. Somehow, with Internet, Bluetooth and any other type of access-related system setting disabled, files are still able to be inserted wirelessly. Also, at least twice this week my third-generation Wi-Fi only iPad battery has drained incredibly fast while turned on, locked, Wi-Fi and other settings turned off, as though someone has been wirelessly infiltrating my device. Also noticeable this week was that on three occasions my iPad was fully off and yet remotely turned on at some point. And, at 11:30 a.m. on Sunday, May 15, a military-looking helicopter flew by my residence about 1000 feet away.

[5] Afternoon of May 13, 2016 at my residence, at which I do not access the Internet at any time.

12. It is peculiar that the Commission's *Second Report and Order and Memorandum Opinion and Order*[6] in May 2006 defined "the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the Drug Enforcement Administration (DEA) (collectively, Law Enforcement)" and LEAs as "law enforcement agencies" referring to CALEA implementation on behalf of the government. The CALEA defined government as "the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance."[7] The CALEA's definition did not mention law enforcement, so in 2006 the Commission neglected to reference the intelligence community, especially the Central Intelligence Agency (CIA) and National Geospatial-Intelligence Agency (NGA).

13. Before continuing with this Comment, I have a message for certain readers: "My life is not as eventful as you seem to believe. Pilots, I've heard and seen you far more than you've heard and seen me; you're not very bright, especially at night. To those who authorized the onslaught of intrusions, what has been accomplished in seven months? What you have been doing, and why, are both ethically and morally wrong."

14. I proceed in this Comment based on two sentences in paragraph 106 and footnote 410 of the *Notice*:

> "Choice is a critical component of protecting the confidentiality of customer propriety information. When armed with clear, truthful, and complete notice of how their information is being used, customers can still only protect their privacy if they have the ability to exercise their privacy choices in a meaningful way."[8]

> "[410] *See* Remarks of FTC Commissioner Maureen K. Ohlhausen, 33rd Annual Institute on Telecommunications Policy & Regulation, December 4, 2015 (arguing that consumers often benefit from the exchange of personal information and that "[a]s long as ISPs, just like others in the internet ecosystem, tell the truth about how they collect and use consumer data, companies should be free to offer different business models and consumers should be free to choose based on their privacy and other preferences.").[9]

15. I present plainly that it is impossible for subscribers of broadband Internet access service (BIAS) to protect against on-going intrusions from unmentionable private sector third parties via government-sponsored monitoring and surveillance. Both the Commission and BIAS providers can not be "clear, truthful, and complete" if the elephant in the room is ignored. The "ability to exercise their privacy choices in a meaningful way" is fundamentally nullified when unaccountable private sector third parties are authorized to have constant access to Customer Propriety Network Information (CPNI) regardless of customer choice.

---

[6] In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket 04-295, FCC 06-56, adopted May 3, 2006, at paras. 1 and 4.

[7] Sec. 102(5), Communications Assistance for Law Enforcement Act of 1994.

[8] Para. 106 of *Notice*, FCC 16-39, adopted March 31, 2016.

[9] *Id.* at para. 263.

III. THIRD PARTY MONITORING AND SURVEILLANCE

16. The machine is not going to stop. The military industrial complex is too complex to diminish. But if the machine is not going to stop, it infuriates discerning people when there is an absence of openness. I have been a passive supporter of Edward Snowden until recently when I discovered the government has been legally enabled via the CALEA[10] for decades.

17. The CALEA's introduction wryly states: "...to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, **and for other purposes**." It seems noteworthy that media has emphasized court orders regarding surveillance, but Section 103(a)(1) specifically states: "pursuant to a court order **or other lawful authorization**" which caused ambiguity for *other* purposes and *other* authorizations to act. What was Edward Snowden uncovering in 2013 but facts that the government took laws that Congress enacted and has pursued utilizing those laws as far humanly and electronically as possible?

18. The U.S. Intelligence Community and, as the Commission defined it, LEAs[11] are fast at work in the global leadership business. As reported last week, Chairman of the Privacy and Civil Liberties Oversight Board, David Meline said at a Senate Judiciary hearing on privacy and government surveillance:[12]

> "The FBI routinely looks into [the Foreign Intelligence Surveillance Act] 702 databases and not just in investigations, but in assessments when the FBI has absolutely no suspicion of wrongdoing."

19. There are citizens and some in Congress alarmed at what is happening, that the government and private sector are not only meshing to where it is too difficult to distinguish, but certain parts of the government have assumed right to intrude on private lives at any time for any reason using the most vulnerable avenues.

20. Section 103(a)(4)(B) of the CALEA mandates that telecommunications carriers can not divulge "information regarding the government's interception of communications and access to call-identifying information." That does not prohibit customer notification that access exists and interceptions occur.

21. The *Notice* lacks substantial meaning if BIAS providers and/or affiliates and/or subsidiaries facilitate monitoring and surveillance to unmentionable third parties that can not be monitored or held accountable. Due to the ambiguity of "other lawful authorization" in Section 103(a)(1) of the CALEA, the door is wide open regarding Section 103(a)(4)(A): "the privacy and security of communications and call-identifying information <u>not authorized</u> to be intercepted."

---

[10] Communications Assistance for Law Enforcement Act of 1994.

[11] In the *Second Report and Order and Memorandum Opinion and Order* in 2006 concerning implementation of the CALEA, the Commission interplayed "CALEA" and "LEAs" when the two were not comparable, mentioning LEAs more than 40 times and not mentioning the word Intelligence once. FCC 06-56, ET Docket 04-295, In the Matter of Communications Assistance for Law Enforcement Act and Broadband Access and Services, adopted May 3, 2006.

[12] *See* article, *Senate Hearing Slams FBI for Indiscriminate Snooping of Foreign Intel*, at http://sputniknews.com/us/20160510/1039392048/fbi-intelligence-is-database.html (May 10, 2016).

22. The CALEA's ambiguous definition of *government* and ambiguous description of *lawful authorization* means that any person or entity can secretly intercept and no one can shine light on who gave the authorization, who committed the interception, why, for what duration, or how the information was handled. In that context, it is mockery to suggest dispute resolution.[13]

A. Microsoft Corporation

23. The following can be found at Microsoft.com:[14]

> "We wanted to protect our customers," says Richard Boscovich, assistant general counsel for Microsoft's Digital Crime Unit (DCU). "As a result, we're hopefully identifying or producing evidence that we can provide to national and international law enforcement so they can not only identify these criminals but apprehend them.
>
> ...Microsoft does something, the gangsters do something, Microsoft does something, the gangsters do something. It's a sophisticated game."
>
> These ripped-from-the-headlines episodes and many others are highlighted at Microsoft's new Cybercrime Center, opening today on the company's Redmond campus. In many ways, the center – and what happens there – is like something straight out of a Hollywood script."

24. Does a consumer really care that Google makes money after clicking an ad? Are people around the world upset because Microsoft can track their moves? A discerning consumer cares when information is or could be used *against* them. Who can do that but those empowered to cause harm or limitations? A rogue hack is like talking about a rogue terrorist attack. It *could* happen, but who knows when, where or the impact? But 24/7 monitoring, as well as surveillance, are directly, continually intrusive; and focus could be placed on me or anyone else at any given moment, and maintained for any given time to arbitrarily thwart, harm or limit a person or entity.

25. The Commission knows well that if subscribers were given the tool to opt out of government surveillance, many would choose yes. That isn't an option, though, so what are you doing? What game is being played as though there is real concern for privacy at the BIAS level? What rule could keep a rogue Microsoft employee from sharing private data obtained via BIAS? How could it be proven that it occurred via a Hollywood-script Cybercrime Center in Redmond, because it can't be revealed to the public?

26. The NPRM's *exclusion* of those as defined in the CALEA who generate, acquire, store, transform, process, retrieve, utilize, or make available information reads like a mockery of the concept of privacy.[15] The government seems to allow privacy to be treated like a hot potato.

> *"This belongs to me—it's private. Okay, sure. Hey, you! Guy across the street! I just took this from someone and you can have it* ***if you'll keep it safe****. Okay, sure. Hey, you! Over there! Someone just gave this to me and I'll sell it to you, but* ***it has to be kept safe****. Sure. Hey! Excuse me, ma'am. I think you could use this. Oh, yes! Okay. Here it is, but you* ***must promise to keep it safe****. Oh, you can count on me, but I won't be able to inform you if something accidentally happens to it. Not a problem, I'm in the same situation."*

27. In 2014, in testimony before the Senate Judiciary Committee regarding botnets and cyber security, FBI's Assistant Director, Cyber Division, Joseph Demarest mentioned the authority by which Microsoft conducted surveillance:[16]

> "In separate but coordinated operations, the FBI, Microsoft, and financial services industry leaders successfully disrupted more than 1,000 botnets built on Citadel malware in a massive global cyber crime operation that is estimated by the financial services industry to have been responsible for over half a billion dollars in financial fraud. Microsoft exercised its independent civil authorities in this matter. The company then coordinated with the FBI and other private parties...."

28. Microsoft exercised its "independent civil authorities," *then* coordinated with the government and other private parties. So, does Microsoft participate in massive global operations for free, or does it directly profit from acting upon independent civil authorities along with other private parties, and do those parties directly link to BIAS providers?

29. If Microsoft and others act upon authorities outside of the CALEA, FISA[17], etc., is it not true those activities can not be defined as "government surveillance"? The Commission should understand if BIAS providers, their affiliates, their subsidiaries, their partnerships and/or their ventures utilize "independent civil authorities" in a manner similar to Microsoft.

B. Comcast Ventures

30. The following is quoted from www.comcastventures.com/network:

> "ACCESS – Unparalleled data and distribution. Comcast Ventures provides a gateway to Comcast Corporation and its residential and business network of 22.4 million video customers, 22.4 million high-speed Internet customers, and 11.3 million voice customers. Over 100 million households view our content through NBCUniversal's brand portfolio.
>
> Our relationship with Comcast and NBCUniversal gives us access to data available nowhere else – in turn, we share that access with our portfolio companies."

31. There are over 100 portfolio companies listed at www.comcastventures.com, and several are listed at http://www.libertyglobal.com/ventures.html: Benu, Bitsight, EdgeConneX, Integrate, and SundaySky.

(Beginning from previous page) ———————————————

[13] Paras. 273-275 of *Notice*, FCC 16-39, adopted March 31, 2016.

[14] *See* article, *Digital Detectives*, at http://news.microsoft.com/stories/cybercrimes/index.html (Nov. 2013).

[15] CALEA, Sec. 102(6)(A).

[16] Testimony of Joseph Demarest, Assistant Director, Cyber Division, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, D.C. on July 15, 2014 at https://www.fbi.gov/news/testimony/taking-down-botnets.

[17] Foreign Intelligence Surveillance Act.

C. In-Q-Tel, Inc.

32. Last month The Intercept published an article providing a link to a brochure from a CEO Summit in California.[18] The brochure describes the host of the meeting:

> "In-Q-Tel (IQT) is the independent, strategic investor for the Central Intelligence Agency and the broader U.S. Intelligence Community. Founded in 1999, IQT is the trusted partner that connects government, startups, and the Venture Capital community to accelerate innovation to further the IC mission."

33. The brochure details that IQT is the third most active corporate investor in four technology areas with more than 300 investments to-date. This year was the 14th annual summit. FBI Director James Comey, as well as Deputy Secretary of Defense Robert Work and National Geospatial-Intelligence Agency Director Robert Cardillo, were speakers. Although now online, the brochure is marked on every page: "© 2016 In-Q-Tel, Inc. Not for further distribution."

34. The "About IQT" portion at www.iqt.org does not mention the CIA.[19] Rather than stating as the brochure that it is "the independent, strategic investor" for the CIA, it instead states that it is "the independent, not-for-profit organization" for the U.S. Intelligence Community with more than 70 percent of its investment portfolio consisting of startup companies that have never before done business with the government. Investments involve the following areas:[20]

> *Collaboration, Communications, Cyber and Mobile Security, Data Management, Data Analytics, Detection and Analysis, Materials and Powers, Video and Imaging*

35. Not only did In-Q-Tel call itself the strategic investor for the CIA, with more than 100 companies listed at its website, but the website for Comcast Ventures calls Comcast Corp. "Our Strategic Investor" with more than 100 companies listed, as well. How can the Commission promote CPNI protection when hundreds of companies have continual access to BIAS subscriber information?

D. Booz Allen Hamilton

36. How can it be so easily found online, from a 2013 article, that 99% of Booz Allen Hamilton's revenue was derived from federal funds, essentially translating to mean a 99% arm of the government?[21] The same CNN Money article detailed:[22]

> "The company earned revenue of $5.7 billion during the last fiscal year and has around 24,500 employees, of which 22,000 are considered to be on the consulting staff. Of those, 76% hold government security clearances, with 49% at "top secret" or higher."

---

[18] *See* article, *The CIA is investing in firms that mine your tweets and Instagram photos*, at https://theintercept.com/2016/04/14/in-undisclosed-cia-investments-social-media-mining-looms-large/?comments=1#comments (April 14, 2016). The brochure face reads CEO Summit 2016 / February 23-25, 2016 / San Jose, CA / www.iqt.org.

[19] https://www.iqt.org/about-iqt/

[20] https://www.iqt.org/portfolio/

37. Intruding on private lives is highly profitable, according to the New York Times:[23]

> "When the United Arab Emirates wanted to create its own version of the National Security Agency, it turned to Booz Allen Hamilton to replicate the world's largest and most powerful spy agency in the sands of Abu Dhabi.
>
> It was a natural choice: The chief architect of Booz Allen's cyberstrategy is Mike McConnell, who once led the N.S.A. and pushed the United States into a new era of big data espionage....
>
> "They are teaching everything," one Arab official familiar with the effort said. "Data mining, Web surveillance, all sorts of digital intelligence collection."
>
> Yet as Booz Allen profits handsomely from its worldwide expansion, Mr. McConnell and other executives of the government contractor—which sells itself as the gold standard in protecting classified computer systems and boasts that half its 25,000 employees have Top Secret clearances....
>
> Removing contractors from the classified world would be a wrenching change: Of the 1.4 million people with Top Secret clearances, more than a third are private contractors."

38. And the website for the National Geospatial-Intelligence Agency (NGA) states:[24]

> "Anyone who sails a U.S. ship, flies a U.S. aircraft, makes national policy decisions, fights wars, locates targets, responds to natural disasters, or even navigates with a cellphone relies on NGA."

39. It was hypocritical for Chairman Wheeler to have included in his Statement for the *Notice*: "And this proposal does not prohibit ISPs from using and sharing customer data – it simply proposes that the ISP *first* obtain customers' express permission before doing so." Every informed person knows express permission will pertain to marketing preferences and the same type of account information safeguards expected in other industries, due specifically to unknown accesses to CPNI by the government and government-sponsored private sector companies.

E. AT&T and Capture IQ monitoring software

40. It is noteworthy that the Webster's New Collegiate Dictionary[25] (© 1941) defines privacy as "1. State of being apart from company or observation; seclusion; also, secrecy. 2. A place of seclusion." That word has been twisted to now mean a kernel of data tossed to and fro just as long as it doesn't fall into unintended hands, determined by someone unknown.

(Continued from previous page) ———————————————

[21] *See* article, *Booz Allen Hamilton in spotlight over leak*, at http://money.cnn.com/2013/06/10/news/booz-allen-hamilton-leak/index.html (June 10, 2013).

[22] *Ibid.*

[23] *See* article, *After Profits, Defense Contractor Faces the Pitfalls of Cybersecurity*, at http://www.nytimes.com/2013/06/16/us/after-profits-defense-contractor-faces-the-pitfalls-of-cybersecurity.html?_r=1 (June 15, 2013).

[24] https://www.nga.mil/About/Pages/Default.aspx

[25] Webster's New Collegiate Dictionary, *Sixth Edition*; copyright 1941, published by Merriam-Webster.

41. In December 2015 The Verge reported that AT&T acquired Capture IQ's phone-monitoring software. The same software that caused scandal and the introduction of the Mobile Device Privacy Act (that didn't pass Congress). In 2011, reportedly 150 million phones had the monitoring software installed without customer knowledge.[26] An AT&T spokesman was quoted regarding the recent acquisition:[27]

> "We've acquired the rights to Carrier IQ's software, and some CIQ employees moved to AT&T...We use CIQ software solely to improve the customer's network and wireless service experience. This is in line with our Privacy Policy and provides a great benefit to users of our network."

42. The spokesman did not say CIQ would improve the network and wireless service, but every customer's experience, more broadly "users of our network." The monitoring software reported to have covered 150 million phones, causing scandal five years ago and congressional response, is now deemed harmless.

43. AT&T's use of CIQ software may conflict with Section 102(8)(C) of the CALEA regarding information services as defined by Section 102(6), if AT&T has not been exempted by rule per Section 102(8)(C)(ii).[28] The *Notice* proposes to define "information services typically provided by telecommunications carriers" in Appendix A § 64.2003 (k), but omits a fundamental exclusion: the CALEA's definition of "information services."

F. Defense Innovation Unit Experimental (DIUx)

44. Last week The Washington Post reported the Pentagon is becoming increasingly involved with Silicon Valley, excerpted:[29]

> "Defense Secretary Ashton B. Carter will overhaul one of his signature efforts, placing new leadership in charge of the Pentagon's office in Silicon Valley just nine months after it opened and directing the staff there to report directly to him. Carter will also establish a sister unit in Boston [home of Skyhook Wireless, acquired by TruePosition, subsidiary of Liberty Broadband, largest stakeholder in Charter Communications], which will also be charged with working with tech companies on concepts with military applications, defense officials said.

---

[26] *See* article, *AT&T acquires part of data collection startup Carrier IQ*, at http://www.theverge.com/2015/12/31/10693478/att-carrier-iq-acquisition-assets-staff-data-collection (Dec. 31, 2015).

[27] *Ibid.*

[28] *See* article, *AT&T Snaps Up Assets, Talent From Carrier iQ, Phone Monitoring Startup Goes Offline*, at http://techcrunch.com/2015/12/30/att-snaps-up-asset-talent-from-carrier-iq-as-phone-monitoring-startup-goes-offline, which suggests AT&T acquired Capture iQ monitoring software accompanied by Nielsen licensing (Dec. 30, 2015). Excerpt: "Nielsen appears to link into the CIQ software also to measure network performance as it relates to services and ads." *See AT&T acquires Carrier IQ software assets and staff*, at http://www.phonedog.com/2015/12/31/att-acquires-carrier-iq-software-assets-and-staff (Dec. 31, 2015). Excerpt: "Back in 2011, there was quite a brouhaha surrounding Carrier IQ when it was discovered that the software was being used on many smartphones and was logging key presses, searches, text messages, and more."

> Carter announced the changes Wednesday at the Silicon Valley office, known in the Pentagon as DIUx, short for Defense Innovation Unit Experimental. The office was launched to build new relationships with technology companies....
>
> A new military unit also will join DIUx. It comprises reservists who work in the tech industry when not serving the Defense Department. It will be led by Doug Beck, a vice president at Apple [customer of Skyhook Wireless] who is a reserve Navy commander, intelligence officer, and combat veteran...."

G. The chilling effect of profit-sharing espionage

45. The CALEA of 1994 did not protect America from 9/11/2001. Existing U.S. laws pertaining to government-sponsored monitoring and surveillances did not prevent the attack in San Bernardino, California, fifteen years after enacting the USA PATRIOT Act. Monitoring en masse has been proven in everyday news to involve both the political and social realms, for secret economic and political gains, as well as squelching and propagandistic diversions. And the 'authorized' third parties providing 'information services' vie for unspeakable bounty.

46. As I conducted personal research it became very clear that the government greatly utilizes the word startup in reference to technology companies. In Hollywood movies it used to be that the CIA operated under fake company names. Now it seems that the government operates in Silicon Valley, Boston, etc., via well-funded "startups" headed by private-sector players.[30]

47. Before the summer of 2013, it could be said without proof that most U.S. citizens were not concerned about government surveillance. However, three years later, in May 2016 the National Telecommunications and Information Administration (NTIA) posted, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*.[31] Analysis was given from a survey conducted in July 2015 by the U.S. Census Bureau. More than 41,000 households that reported having at least one Internet user were asked about privacy and security. It seems identity theft is a major concern, but the following are two excerpts:[32]

> "29 percent of households concerned about government data collection said they did not express controversial or political opinions online due to privacy or security concerns...."
>
> "NTIA's initial analysis only scratches the surface of this important area, but it is clear that policymakers need to develop a better understanding of mistrust in the privacy and security of the Internet and the resulting chilling effects. In addition to being a problem of great concern to many Americans, privacy and security issues may reduce economic activity and hamper the free exchange of ideas online."

(Continued from previous page) ———————————————

[29] *See* article, *Pentagon chief overhauls Silicon Valley office, will open similar unit in Boston*, (May 11, 2016) at https://www.washingtonpost.com/news/checkpoint/wp/2016/05/11/pentagon-chief-overhauls-silicon-valley-office-will-open-similar-unit-in-boston. *See also* http://www.diux.mil.

[30] *See* footnote 18. The brochure reads: "Founded in 1999, IQT is the trusted partner that connects government, startups, and the Venture Capital community...."

[31] *Available at* https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (May 13, 2016).

48. To emphasize the sentiment, Engadget.com picked up on that post and began an article by stating: "Have countless data breaches and unfettered government surveillance left you nervous about doing things online? You're definitely not alone."[33]

49. In-Q-Tel (IQT, CIA's independent strategic investor) maintains several articles at its website, including one titled *Social Media Technologies* by Bruce Lund. Excerpted:[34]

> "...applications may eventually be adopted by government agencies to track epidemics, disasters, and emerging political movements on a global scale."
>
> "Key reasons to monitor social media as close to real-time as possible include:
>
> - Improving the analysis of potential indicators of societal change as well as informing predictive analysis.
> - Understanding the source and direction of trending topics by measuring how ideas spread in social networks."

H. Skyhook Wireless, acquired by TruePosition, owned by Liberty Broadband, Largest Stakeholder in Charter Communications

50. Emarketer.com posted an article in November 2015, *Mobile App Users Reluctant to Share Location*, excerpted:[35]

> "Privacy and security are critical to mobile users, most of whom have some understanding of how revealing their mobile data—including location—can be to advertisers, publishers, governments and other internet users. And for many, that means not using location services at all, potentially diminishing their mobile experiences.
>
> According to research from mobile location services provider Skyhook Wireless (http://www.skyhookwireless.com/), US mobile app users are more likely to turn on location services for weather apps than for any other category—but even then, when the utility of location-sharing is obvious, 35% of app users refuse to do so.
>
> For other app categories, the share of users who enabled location services was even lower, dropping to 16% for news apps—another category where specifying location would seem useful in bringing users local stories, for example.
>
> ...Earlier research found that nearly eight in 10 US internet users worried smart devices would reveal their location without their knowledge."

51. The concern that location could be revealed without user knowledge was written in an article ironically mentioning research conducted by Skyhook Wireless. For MB Docket 15-149 (Charter-TWC-BHN joint applications), I mentioned what was stated at Skyhook Wireless' website.[36] The Commission should understand Skyhook's "Personas" mentioned at their website.

(Continued from previous page) ————————————————

[32] *Ibid.*

[33] *See* article, *Data breaches and spying fears are keeping people offline*, at http://www.engadget.com/2016/05/14/data-breaches-and-spying-create-chilling-effect (May 14, 2016).

52. Quoted from Skyhook's website:

> "Skyhook's massive global network powers billions of location requests in all of the places that they happen. Our customers include giants like Apple, Samsung, Sony and Mapquest. Our coverage is monumental and constantly growing."
>
> "Skyhook's Personas unlock mobile consumer behavior – their demographics, interests, and intents – based on location history. Our out-of-the-box Personas are market-ready for you to customize content or pass anonymized user data to your advertisers or other 3rd party partners."
>
> "Geospatial Insights is a view into consumer foot traffic around the world based on hundreds of billions of location samples. Analyze quantifiable data from our 100-by-100-meter tiles that cover the globe, delivered in hourly buckets. Our customers monitor mobile activity levels in areas they select for financial intelligence, media planning, and retail strategy."

53. The Commission seeks comment via paragraphs 43 and 44 of the *Notice* whether device geo-location and other identifiers should be deemed CPNI. The following is also from Skyhook's website:

> "Skyhook understands that consumers care about privacy and goes to great lengths to protect it. We do not collect names, home addresses, email addresses, etc. We build Personas by associating anonymous device IDs with location information and other anonymized demographic attributes, instead of with any personally identifiable information. Skyhook also observes many layers of opt-out preferences in the OS, app, and advertising settings, giving consumers the ultimate choice of how their information is used."

54. But all it takes for a device to be linked to an individual is for someone to inform. That is exactly what happened to me when Charter Communications either directly or indirectly provided my laptop and iPad IDs to one or more third parties, who then subjected me to on-going surveillance for seven months. I mentioned that via MB Docket 15-149, as well.[37]

55. TruePosition acquired Skyhook in 2014, and TruePosition's website states:[38]

> "TruePosition, the Location Specialists. No other company matches our breadth and depth of experience or our industry leading product portfolio."
>
> "[TruePosition's TrueFix location platform] offers: Security, privacy and accountability not available from the major operating system suppliers...."

(Continued from previous page) ———————————————

[34] *Available at* https://www.iqt.org/technology-focus (downloadable PDF) IQT Quarterly, Vol. 3 No. 3, at pg. 3.

[35] http://www.emarketer.com/Article/Mobile-App-Users-Reluctant-Share-Location/1013276 (Nov. 25, 2015).

[36] Filings which mentioned Skyhook Wireless: November 12, 2015 Reply to Responses/Oppositions at pgs. 28-29; December 27, 2015 Supplemental Reply to Responses/Oppositions at pgs. 14-15; April 11, 2016 Letter at pgs. 3-5.

[37] April 17, 2016 Letter at 7, filed electronically. The Commission rightfully proposes in Appendix A § 64.2003 (o) of the *Notice* to define *Personally Identifiable Information* as both linked and linkable.

[38] *See* http://www.trueposition.com *and* http://www.trueposition.com/products/truefix-platform.

56. Section 103(a)(2)(B) of the CALEA specifically envisioned technological ability to locate an individual within small perimeters.[39] It also provided restriction against such ability:

> "...with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."

57. A telephone number, with identifying area code and prefix, is not a device ID that can be pinpointed via cellular and/or Wi-Fi signals. And when the CALEA was enacted, devices such as a Wi-Fi only iPad were mostly inconceivable; but yet monitoring and surveillance has extended to such devices that do not even involve a phone number. I am an example. I do not own a phone, but yet I am under surveillance via a Wi-Fi only iPad able to be located instantly when the device begins searching for available signals, and through other methods.

58. With the Commission's *Notice* omitting contemplation of both government and third party monitoring and surveillances, how can you obtain understanding of declarations such as made by TruePosition that they provide "security, privacy and accountability" not available by Apple, Google or Microsoft? How do their pervasive operations remain separate of CPNI? Does Skyhook Wireless maintain profiles ("Personas") for every device ID in America, and beyond?

IV. CUSTOMER NOTIFICATION

59. Regarding Appendix A § 64.2011 (a) of the *Notice*, the Commission could better serve subscribers of BIAS by mandating a choice as to whether breach notifications are sent via U.S postal mail or electronic mail. As it reads in the *Notice*, the BIAS provider would be allowed to choose "any of the following methods" which includes "other electronic means," rather than giving subscribers the right to choose. This reminds me of the language contained in the current *Residential Internet Service Agreement* for Charter Communications (Charter):

> "19. Amendment: Charter may, in its sole discretion, change, modify, add or remove portions of this Agreement at any time. Charter may notify Subscriber of any such changes by posting notice of such changes on Charter's website at www.charter.com, under "Terms of Service/Policies", or sending notice via electronic mail or U.S. postal mail." The Subscriber's continued use of the Internet Service following notice of such change, modification or amendment shall be deemed to be the Subscriber's acceptance of any such modification."

60. Charter allows itself to provide all notifications of changes to terms of service via subscriber mailing addresses, email addresses, or simply by posting online. Absent restrictions or preferences, that same methodology could be applied to breach notifications.[40]

---

[39] *i.e.,* www.skyhookwireless.com states: "We position your users down to 20 meters and deliver location 99.8% of the time."

[40] Para. 89 of the *Notice*—Compliance Burden—the burden would depend on preferences for U.S. postal mail.

61. The Commission seeks comment on imposing a standardized privacy notice,[41] and I suggest both imposing essentials for the notice and providing guidance for such as Section 103(a)(4)(B) of the CALEA—distinguishing between details of access and interceptions of the government and providing summaries of the BIAS provider's lawful obligations. Or, instead of guidance, provide standardized summaries of pertinent law as part of the essential information. As an interested person, I suggest the following be included in BIAS providers' privacy notice:

- Types of information that BIAS providers are required by law to allow access.
- The U.S. government monitors subscribers and other consumers based on law.
- Authorized surveillance occurs at the government's non-disclosed discretion.
- Monitoring is and authorized surveillance may be conducted by authorized non-governmental (private) parties in addition to government agencies.
- List of every law that authorizes the government to both monitor en masse and conduct authorized individual-based surveillance.
- Summary of the purposes for government monitoring and surveillance, which primarily involve the intelligence community and law enforcement agencies.[42]
- Services by which monitoring is conducted (e.g., video (including via satellite), voice, and/or Internet services), as well as affected types of devices.

62. Regarding when the privacy notice should be given,[43] in addition to encouraging applicants during the ordering process to read the Privacy Policy at the BIAS provider's website, a printed privacy notice, which excludes other information, could easily be given to applicants at the time of installation, as well as supplied again with the initial, mailed billing statement.

V. DEFINING CUSTOMER

A. Applicants for broadband Internet access service

63. Last week I was at a grocery store register and someone walked in and handed the clerk a job application and left. I glanced at the logo at the top of the application and mentioned to the distracted clerk it was for the wrong store. Was that store obligated to keep the information secure? Surely a BIAS provider is competent enough without intervention to keep non-customer applicant information for BIAS—handled via a phone call or otherwise—safeguarded, shredded or deleted.

64. Paragraph 31 of the *Notice* proposes to partly define "customer" as an applicant, but that is incongruous. If an applicant for BIAS ends the relationship before installation begins, when did the applicant convert to a customer? The terms which applicants subscribe to during the order process become null and void if the relationship ends before the service is activated. Only after BIAS installation, when service is active—regardless of payment or use of service—does "applicant" convert to "customer." The Commission should not define a new applicant as "customer" in the same context as one whose service is activated.

---

[41] Regarding paras. 89-91 of the *Notice*—Compliance Burden *and* Standardization of Privacy Notices.

[42] The CALEA begins by stating: "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, *and for other purposes*."

B. Former subscribers

65. The Commission's proposal to define customer to mean 'current or former, paying or non-paying subscriber to BIAS' should not be imposed separate from BIAS providers updating their terms of service. And I, as a former subscriber, do not expect that non-consented terms will affect me. Imposing retroactive protections absent former subscribers' consent could result in a number of tussles.

66. Former subscriber information must be maintained by BIAS providers, such as Charter Communications, due to surviving provisions in terms of service. For example, Charter's current general terms and conditions read online:[44] "The foregoing arbitration provisions shall survive the termination of this Agreement." Therefore Charter, for instance, maintains applicable former subscriber information partly due to that clause. But it is reasonable to incorporate former subscribers as "customer" after terms and conditions for broadband service have been updated to include surviving provisions for privacy protection, etc.

67. Also, if the proposed term "non-paying" is included in the definition of customer, without clarification "non-paying subscriber" could be interpreted to include entire households. To avoid any broad interpretation, the Commission should ***replace*** "paying or non-paying" with "active or inactive" and/or "person or entity".[45] Otherwise, a door could open for far-reaching interpretations.

C. Confusion caused by 'customer', 'subscriber' interplay

68. Since I am a former subscriber of Charter Communications who received Internet service, I will use their current terms of service posted at www.charter.com as an example. In the *General Terms and Conditions for Charter Residential Services* agreement, the accountholder is termed "You ("Subscriber")" while the word customer is used 15 times. More specifically, of the 15 uses, 5 are for the Limitation of Liability clause in which "Subscriber" is not used at all. Throughout the Agreement Charter capitalizes Subscriber but leaves customer lowercase; but in the Limitation of Liability clause, for instance, every letter is capitalized. So Charter utilizes "You ("Subscriber")", "Subscriber", "customer" and "CUSTOMER" for terms of service.

69. Historically, when I obtained service from Charter in 2013, the *Charter Internet Residential Customer Agreement* stated:[46]

> "This Service Agreement ("Agreement") states the terms and conditions under which Charter Communications, Inc. and its subsidiaries (collectively "We" or "Charter") will provide the Service to a subscriber ("You" or "Customer")."

(Continued from previous page)

[43] Para. 82 of the *Notice*—Providing Meaningful Notice of Privacy Policies.

[44] *See* section 24, *General Terms and Conditions for Charter Residential Services*, available at www.charter.com.

[45] Appendix A § 64.7000(e)(1) of the *Notice*.

[46] Quoted from a PDF made in July 2014 of the *Charter Internet Residential Customer Agreement*. At charter.com the agreement was described as "Effective April 2008. Version 8.2."

70. For the Introduction of the *Notice*, 'consumer' was used 30 times, 'customer' 14 times, and 'subscriber' only twice. Webster's New Collegiate Dictionary[47]—© 1941, just seven years after the Communications Act was enacted—defined subscriber: "**1.** To sign one's name to a document. **2.** To give one's consent in or as in writing; often, to express assent;—usually with *to*; as, I *subscribe* to that statement. **3.** To set down one's name as token of a promise to give something, as money; also, loosely, to give something in accordance with such a promise. **4.** To agree to take and pay for something, as stock, or a journal, esp. by signing a formal agreement."

71. "Customer" and "Subscriber" are not entirely synonymous, because a *subscriber* can be bound to surviving provisions of a formal agreement. In the context of Section 222 of the Communications Act, defining a subscriber as "customer" is conflicted by BIAS providers, such as Charter, whose terms of service were updated from "Customer" to "Subscriber". If providers must adhere to the word customer in rules and law, should they not also use that word in their terms of service? Perhaps they can't get away from using "subscriber" because of the CALEA.

72. When the CALEA was enacted the words customer and subscriber were used for separate definitions in Section 102. The subscriber related to call-identifying information, but the customer related to information services. In Section 103 the phrases "customer or subscriber" and "subscriber or customer" were used. And Section 207 again separated the terms, stating "a subscriber to or customer of such service and the types of services the subscriber or customer utilized." So, the CALEA distinguished subscribers and customers, defining *subscriber* as one generating or receiving communications and *customer* as a third-party handler of information.[48]

73. The CALEA caused confusion, because *customer* should not have been confined to information services. On the other hand, Sec. 2510 of the Electronic Communications Privacy Act (ECPA) of 1986 caused confusion because it stated "subscriber or user"[49] and then defined user as follows:

> (13) "user" means any person or entity who—
> (A) uses an electronic communication service; and
> (B) is duly authorized by the provider of such service to engage in such use [50]

74. In order for someone to use free, public Wi-Fi service provided, for example, by AT&T, a person agrees to terms and conditions linked to the initial connection screen. However, a person regularly using someone else's private service without the BIAS provider's knowledge is incapable of being "duly authorized" to use the service. Who is a "user" in the BIAS context?

75. The public interest would be served by acknowledging these nuances that directly impact CPNI as the Commission seeks to alter the definition of "customer" for Section 222.[51] Another aspect is whether the CALEA or ECPA involve both applicants and former subscribers.

---

[47] Webster's New Collegiate Dictionary, *Sixth Edition*; copyright 1941, published by Merriam-Webster.

[48] Sec. 102(2) and (6).

[49] 18 U.S.C. § 2510(5)(a)(i).

[50] 18 U.S.C. § 2510(13).

[51] 47 U.S.C. § 222(h).

VI. DISPUTE RESOLUTION MECHANISM

76. Paragraph 273 of the *Notice* regards dispute resolution with the question: "Are these mechanisms adequate?"[52] It is a wake-up call for the Commission to read the Limitation of Liability clause in the terms currently maintained by Charter Communications:[53]

> "22. LIMITATION OF LIABILITY. THE LIMITATION OF LIABILITY SET FORTH IN THIS SECTION APPLY TO ANY ACTS, OMISSIONS AND NEGLIGENCE OF CHARTER AND ITS THIRD-PARTY SERVICE PROVIDERS, AGENTS AND SUPPLIERS (AND EACH OF THEIR RESPECTIVE OFFICERS, EMPLOYEES, AGENTS, CONTRACTORS OR REPRESENTATIVES).
>
> UNDER NO CIRCUMSTANCES SHALL CHARTER BE LIABLE TO CUSTOMER FOR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE SERVICE OR ANY ACTS OR OMISSIONS ASSOCIATED THEREWITH, INCLUDING ANY ACTS OR OMISSIONS BY THIRD-PARTY SERVICE PROVIDERS, AGENTS OR SUBCONTRACTORS OF CHARTER, OR RELATING TO ANY SERVICES FURNISHED, WHETHER SUCH CLAIM IS BASED ON BREACH OF WARRANTY, CONTRACT, TORT OR ANY OTHER LEGAL THEORY, AND REGARDLESS OF THE CAUSES OF SUCH LOSS OR DAMAGES OR WHETHER ANY OTHER REMEDY PROVIDED HEREIN FAILS. CHARTER'S ENTIRE LIABILITY AND CUSTOMER'S EXCLUSIVE REMEDY WITH RESPECT TO THE USE OF THE SERVICES OR ANY BREACH BY CHARTER OF ANY OBLIGATION CHARTER MAY HAVE UNDER THESE TERMS OF SERVICE OR APPLICABLE LAW, SHALL BE CUSTOMER'S ABILITY TO TERMINATE THE SERVICE OR TO OBTAIN THE REPLACEMENT OR REPAIR OF ANY DEFECTIVE EQUIPMENT PROVIDED BY CHARTER...."

77. Who can come against such an impenetrable blockade of accountability other than the government? I digress to mention that termination is neither redress nor corrective, though implied as remedy. Nevertheless, that is the language that must be addressed if subscribers are to expect meaningful resolutions.[54] How can the Commission mandate privacy protections in the public interest when one or more major BIAS providers evade basic accountability? The FCC should not be in delusion concerning BIAS providers such as Charter Communications, for prior to October 1, 2014[55] Charter's Limitation of Liability clause contained the language as follows.

(Continued from previous page) ———————————————

[52] Paras. 68-70; also, item 8 of para. 27.

[53] *See* sec. 22 of *General Terms and Conditions for Charter Residential Services* at www.charter.com.

[54] Para. 27 of the *Notice*: "...ensuring BIAS customers have meaningful choice about the use and disclosure of their customer PI...." Also, the excerpt in footnote 173 of the *Notice* from Kamala D. Harris, Attorney General, California Department of Justice suggests a "simpler, shorter privacy notice". Who seeks that? Not much of the public. The public doesn't read it, or want to, because it's predominantly untrustworthy jargon. Much of American society is now savvy and/or wary, not trusting that the government tells the truth, the whole truth and nothing but the truth.

[55] Quoted from a PDF made in July 2014 of the *Charter Communications Terms and Conditions of Residential Service ("Agreement")* at www.charter.com.

> [removed effective October 1, 2014] "...WITHOUT ABROGATING OR OTHERWISE LIMITING THE FOREGOING LIMITATION, IN THE EVENT OF GROSS NEGLIGENCE (OR EQUIVALENT BEHAVIOR) OR WILLFUL MISCONDUCT BY CHARTER, ITS SUPPLIERS, EMPLOYEES, AGENTS OR CONTRACTORS, WE MAY PAY AT OUR SOLE DISCRETION A MAXIMUM OF $500. THIS SHALL BE YOUR SOLE AND EXCLUSIVE REMEDY RELATING TO SUCH ACTIVITY...."

VII. DEFINING TELECOMMUNICATIONS CARRIER OR CARRIER

78. In my lack of formal education I could be mistaken, but Appendix A § 64.2003 (r) of the *Notice*, for the definition of telecommunications carrier or carrier, reads as though there is a grammatical error or a dramatic intention. Is it true that a telecommunications carrier or carrier "shall exclude an entity that provides broadband Internet access service"? If so, would that mean that any telephone company that begins providing BIAS would suddenly switch categories?

VIII. CONCLUSION

79. Paragraph 33 of the *Notice* suggests that consumers may be hesitant to switch providers out of concern that their current provider may stop protecting their privacy after the switch. When Edward Snowden brought global attention to mass monitoring, both Verizon and AT&T became prominently emphasized. Rather than assuming consumers are hesitant to switch providers due to fear that a previous may stop protecting them, it can just as easily be assumed there is fear of switching to a provider, such as AT&T or Verizon, that may vanquish privacy, whether real or perceived. Notwithstanding, many consumers are simultaneous customers of AT&T for cellular and/or video service and Charter Communications for Internet service.

80. In February, The Hill published an article regarding the FCC's upcoming *Notice* which quoted the following from a representative of USTelecom:[56]

> "Well, I think essentially, the key point is that consumers have certain expectations as to how their private information will be treated," said Lynn Follansbee, a vice president for law and policy at USTelecom, which represents broadband providers. "And we just take a position that no matter, across the whole Internet ecosystem, no matter what kind of technology is involved, consumers shouldn't be surprised."

81. Although USTelecom "represents broadband providers" the comment "consumers shouldn't be surprised" is fundamental. The scope of the *Notice* is insufficient, because it doesn't acknowledge the true picture of "who, what, when, where and why" CPNI is acquired, stored, transformed, processed, retrieved, utilized, or made available to and by third parties—including proposed information to be assimilated into the definition of CPNI, such as geo-location.[57] In light of information contained in this Comment, the Commission should not unequivocally deny contemplation of what occurs on a regular basis, but instead be clear, truthful, and complete.[58]

---

[56] *See* article, *FCC poised to flex new privacy powers*, February 15, 2016, at http://thehill.com/policy/technology/269337-fcc-poised-to-flex-new-privacy-powers.

[57] Paras. 41 and 43 of the *Notice*.

[58] Para. 106 of *Notice*.